

ABSTRACT

Method and device for secure wireless transmission of information from a sender to a receiver. A sending device is arranged for obtaining a message, a sender identity and a receiver identity and includes encryption means for encrypting the message to be transmitted. A transmission channel is established from the sending device to a receiving device for transmitting the encrypted information to the receiving device. A secure note is used for defining the receiving device. In the receiving device, there is arranged decryption means for decrypting the information and display means for presenting the message to the receiver. Optionally, the receipt of the message is verified to the sender. Preferably, the message is encrypted in the sending device by a symmetric key and decrypted by the receiving device by the same key. The symmetric key is added to the message after encryption with the symmetric key and the symmetric key is encrypted by a public key belonging to the receiver, whereupon the already encrypted symmetric key is encrypted by a private key belonging to the sender. In the receiving device, the symmetric key is decrypted by the public key of the sender in the receiving device and by the private key of the receiver, whereupon the symmetric key is used for decrypting the message. The sender and the receiver identifies themselves to the sending device and the receiving device by verification means. Preferably, a random seed for generating encryption key is obtained by the verification means during the identification step and/or the message step. Preferably, the sending device is an Anoto pen.